REMARKS

I. INTRODUCTION

In response to the Office Action dated March 28, 2006, claims 1, 2, 7, 8, 10, 11, 16, 17, 19, 20, 24, 25, 26, 28, 29, 33, 34, and 35 have been amended. Claims 1-36 remain in the application. Entry of these amendments, and re-consideration of the application, as amended, is requested.

III. PRIOR ART REJECTIONS

In paragraph (5) of the Office Action, claims 19, 20, 22, 23 and 26 were rejected under 35 U.S.C. §102(e) as being anticipated by Kocher, U.S. Patent 6,289,455 (Kocher). In paragraph (11) of the Office Action, claims 1, 2, 4, 5 and 8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen, U.S. Patent 5,282,249 (Cohen) in view of Kocher. In paragraph (17) of the Office Action, claims 3, 6 and 7 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen in view of Kocher, and further in view of Pitts, U.S. Publication 2002/0145931 (Pitts). In paragraph (21) claim 9 is rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen in view of Kocher, and further in view of Barth, U.S. Patent 6,334,216 (Barth). In paragraph (23) of the Office Action, claims 10, 11, 13, 14, 17, 18, 27-29, 31, 32, 35 and 36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kochet in view of Barth.

Applicants respectfully traverse these rejections.

Specifically, the independent claims were rejected as follows:

> As per claim10, Kocher discloses a method for limiting unauthorized access to digital services comprising:
>
> Embedding a hidden non-modifiable identification number into a nonvolatile memory component (column 21 lines 13-15 and column 18 lines 37-45 wherein the identification number is the serial number alluded to and which is stored in the protected memory and is non-modifiable in the same manner as the unique BATCH_KEY described in column 18 lines 49-52; see also claim 1), wherein:
>
> The nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv);
>
> The hidden non-modifiable identification number uniquely identifies a device containing the nonvolatile memory component (column 18 lines 37-45 see also claim 1); and
>
> the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9 and column 18 lines 37-45 and column 26 lines 25-40); It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copied to another CAM. These

PAGE 13/16 * RCVD AT 6/23/2006 6:56:57 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/15 * DNIS:2738300 * CSID:3109640941 * DURATION (mm-ss):05-06

passages clearly demonstrate that a compromised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by Applicant where if an identification number is known to be used by multiple devices illegally, those devices using that number would no longer be effective); and

Isolating access to the nonvolatile memory component such that access to the nonvolatile memory component is limited to a fixed state custom logic block (Fig. 2 #260 where in the CryptoFirewall is the custom logic block as described in column 21 lines 34-35), the nonvolatile memory component is protected such that the nonvolatile memory component is not directly accessible via a system bus (Fig. 2 #260).

But does not disclose wherein access to the digital services is based on access rights associated with the hidden non-modifiable identification number.

Barth does disclose wherein access to the digital services is based on access rights associated with an identification number (column 4 lines 33-45 wherein the access rights is whether it is associated with a blocking note).

Barth is analogous art because it discloses a method of gaining access to services based on an identification number utilized in an access card.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Kocher to include the method of comparing an identification number to a list of unauthorized number and their access rights before granting access.

Motivation for one to modify Kocher as discussed above would have been to allow system management to prevent access to the services if the corresponding number is reported as lost or if the user is delinquent in his obligations for the services offered as taught in Barth (column 3 lines 37-42).

As to claim 19, Kocher discloses a conditional access module (CAM), (Fig. 2 #255 wherein the CAM is the cryptographic rights unit) comprising:

a nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv; and

the nonvolatile memory component is protected from modification such that the nonvolatile memory component is read only (column 10 lines 43-47); and

access to the nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the non-volatile memory component, wherein the identification number embedded into the nonvolatile memory component, where the identification number uniquely identifies the CAM (column 7 lines 65-67 column 10 lines 38-40 and 43-45: it can be understood that the device key necessarily applies to an identification number which as used by the applicant is a security-related parameter. Moreover, in view of column 10 lines 61-65 and column 11 lines 53-65 it can clearly be seen that the rights key which is generated from the device key/identification number is used to decrypt/access the content; which meets the functionality of the identification number as defined by the Applicant. Moreover in column 12 lines 24-32, 37-40 and 62-66, Kocher explains the use of the device key to determine permission of access to the services, which also meets a requirement of the identification number as stated by the Applicant); and

the identification number is used to limit a cloning attack where said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9 and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copied to another CAM. These passages clearly demonstrate that a comprised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by the Applicant wherein if an identification number is known to be used by multiple devices illegally, those devices using that number would no longer be effective); and

a fixed state custom logic block, where the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

Independent claims 1, 10, 19 and 28 are generally directed to the use of an identification number. Specifically, the claims address an identification number that is used to limit a cloning attack. As set forth throughout the specification (including paragraphs [0062], [0072]-[0074], and [0078]), the identification number uniquely identifies the device (i.e., the CAM) and such an identifier is used in a particular context. In this regard, the amended claims specifically provide that the identification number is used to limit a cloning attack wherein such a cloning attack comprises copying the identification number to a new pirated CAM. As indicated in the specification, hacking techniques typically use a low cost cloning attack wherein the identity of a pirate card is copied to a new card. The claims provide for hiding this identification number in the isolated nonvolatile memory component. By preventing access to the identification number (except through the custom logic block), the low cost cloning attack techniques are limited. Neither of the cited references teach nor suggest these various elements of Applicants' independent claims.

In addition, Applicants note that the amended claims provide additional limitations. Namely, the claims now provide for two nonvolatile memory components. One nonvolatile memory component is protected and contains the hidden number as described above. The other nonvolatile memory component is unprotected and is referred to as a microprocessor's unprotected nonvolatile memory component. The claims provide specific limitations and details regarding both the protected and unprotected nonvolatile memory components. In this regard, the amended claims provide that programming control and a programming charge pump are shared by both nonvolatile memory components. The specification paragraph [0070] describes the advantages of sharing programming control and a charge pump:

> **[0070]** Additionally, the two nonvolatile memory components 606 may share programming charge pumps and programming control. If the pumps and/or programming control are shared, care should be taken to ensure that data and address lines of the nonvolatile memory component 606 containing the hidden number 614 are routed only to the custom logic block 612. This saves chip area and reduces chip cost. Accordingly, the microprocessor 602 cannot provide control information that may lead to a subsequent attack on the protected/dedicated memory component 606 (i.e., the component containing the hidden number 614). Sharing the charge pumps may be preferred to ease timing and high voltage requirements of the entire chip within CAM 512.

Thus, there are distinct and clear advantages to sharing programming control and a charge pump between the two nonvolatile memory components. Such advantages and limitations are clearly missing and not even remotely alluded to in Kocher or the other cited references. In fact, an electronic search of Kocher for the term "charge" merely provides results for charging users for

PAGE 15/16 * RCVD AT 6/23/2006 6:56:57 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/15 * DNIS:2738300 * CSID:3109640941 * DURATION (mm-ss):05-06

purchases. Further, an electronic search of Kocher for the term "pump" provides no results whatsoever. Without even mentioning a programming charge or a charge pump, Kocher cannot possibly teach the detailed and specific limitations of the amended independent claims.

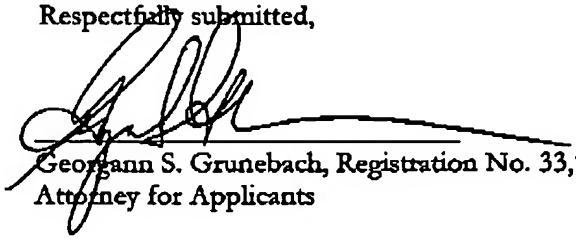
Further, Cohen, Pitts, and Barth also fail to cure Kocher's deficiencies. The various elements of Applicants' claimed invention together provide operational advantages over the systems disclosed in Kocher, Cohen, Pitts, and Barth. In addition, Applicants' invention solves problems not recognized by Kocher, Cohen, Pitts, and Barth.

Thus, Applicants submit that independent claims 1, 10, 19 and 28 are allowable over Kocher, Cohen, Pitts, and Barth. Further, dependent claims 2-9, 11-18, 20-27 and 29-36 are submitted to be allowable over Kocher, Cohen, Pitts, and Barth in the same manner, because they are dependent on independent claims 1, 10, 19 and 28 respectively, and because they contain all the limitations of the independent claims. In addition, dependent claims 2-9, 11-18, 20-27 and 29-36 recite additional novel elements not shown by Kocher, Cohen, Pitts, and Barth.

IV. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,



Georgann S. Grunebach, Registration No. 33,179
Attorney for Applicants

Date: June 23, 2006

The DIRECTV Group, Inc.
RE / R08 / A109
P.O. Box 956
2230 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: (310) 964-4615

PAGE 16/16 * RCVD AT 6/23/2006 6:56:57 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/15 * DNIS:2738300 * CSID:3109640941 * DURATION (mm-ss):05-06